

## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for managing a peer-to-peer collaboration system, the method comprising:
  - (a) using client software operating in a first device and a second device to connect a first user of the first device to a second user of the second device in a peer-to-peer collaboration session including the first user and second user, the first user having a first collaboration identity in a shared space and the second user having a second collaboration identity in the shared space;
  - (b) downloading from the management server to the client software operating in the first device a definition file containing a definition of a managed entity;
  - (c) associating a management identity in the definition file with the first collaboration identity or first device information in the client software operating in the first device in order to create the managed entity, the management identity associated with the managed entity being different than the first collaboration identity, the management identity allowing the first user or first device to be identified by the management server;
  - (d) interacting, between the management server and the client software using the management identity, to exchange management information associated with the operation of the managed entity in the peer-to-peer collaboration session separately from the collaborative information exchanged between the first user and the second user, wherein the exchanged management information comprises at least a ~~license file and/or~~ a policy restriction file, wherein interacting further comprises:
    - i) creating a client list of policy restrictions in the client software of the managed user;
    - ii) sending the client list to the management server;
    - iii) creating a server list of policy restrictions in the management server;
    - iv) comparing the client list to the server list; and

- v) adjusting and synchronizing the policy restrictions in the client software based on the comparison on step iv); and
- (e) ~~if the exchanged information includes a policy restriction file,~~ in response to information in the policy restriction file, restricting at least one function in the client software.
2. (Previously Presented) The method of claim 1 wherein the managed entity is a managed user and the definition file is an injectible identity file and the act (c) of associating comprises incorporating information from the injectible identity file into a user account file.
3. (Previously presented) The method of claim 1 wherein the managed entity is a managed device and the definition file is a device information file.
4. (Previously Presented) The method of claim 3 wherein the act (c) of associating comprises incorporating information from the device information file into a Windows REG file.
5. (Canceled).
6. (Currently Amended) The method of claim 1, wherein the exchanged information is a ~~policy restriction file~~ license file and interacting comprises in response to information in the ~~policy restriction~~ license file, ~~restricting at least one function in the client software~~ and the method further comprises enabling at least one function in the client software.
- 7.-9 (Canceled)
10. (Previously Presented) The method of claim 1 wherein steps i) to v) are repeated periodically.

11. (Previously presented) The method of claim 1, wherein the management information comprises event notifications and statistical information and interacting to exchange management information comprises:

- i) periodically sending the event notifications and the statistical information from the client software of the managed user to the management server.

12. (Original) The method of claim 11 wherein the event notifications include error notifications.

13. (Original) The method of claim 11 wherein event notifications and statistical information are temporarily stored in a memory located at a client site.

14. (Currently Amended) Apparatus for managing a peer-to-peer collaboration system, the apparatus comprising:

client software operating in a first device and a second device, the software connecting a first user of the first device to a second user in a peer-to-peer collaboration session including the first and second users, the first user having a first collaboration identity in a shared space and the second user having a second collaboration identity in the shared space;

a download manager that downloads from the management server to the client software operating in the first device a definition file containing a definition of the identity of a managed entity;

a mechanism in the client software that associates the definition with the first collaboration identity or first device information in order to create the managed entity, the management identity associated with the managed entity being different than the first collaboration identity, the management identity allowing the first user or first device to be identified by the management server; and

a mechanism that exchanges information relating to the managed entity between the client software and the management software using the management identity, the information relating to monitoring operation of the managed entity and/or synchronizing the managed entity

with information on the management server, the exchanged information being associated with the identity of the managed entity, wherein:

the exchanged management information comprises at least ~~a license file and/or a~~ policy restriction file; and

~~if the exchanged information includes a policy restriction file, the apparatus is~~ adapted to, in response to information in the policy restriction file, ~~restricting~~ restrict at least one function in the client software.

15. (Previously presented) The apparatus of claim 14 wherein the managed entity is a managed user and the definition file is an injectible identity file.

16. (Previously presented) The apparatus of claim 14 wherein the managed entity is a managed device and the definition file is a device information file.

17. (Original) The apparatus of claim 16 wherein the device information file is a Windows REG file.

18. (Canceled).

19. (Previously Presented) the apparatus of claim 14, wherein the mechanism that exchanges information comprises:

policy control software in the management server that sends at least one policy restriction file from the management server to the managed user; and

policy control software in the client software that, in response to information in the policy restriction file, restricts at least one function in the client software.

20. (Previously Presented) The apparatus of claim 14, wherein the mechanism that exchanges information comprises:

management software in the management server that creates a client list of policy restrictions in the client software of the managed user;  
a transport mechanism that sends the client list to the management server;  
management software in the client software that creates a server list of policy restrictions in the management server;  
a mechanism that compares the client list to the server list; and  
a mechanism that adjusts and synchronizes the policy restrictions in the client software in cooperation with the comparison mechanism.

21.-22 (Canceled).

23. (Previously Presented) The apparatus of claim 20 wherein the adjusting and synchronizing mechanism operates periodically.

24. (Previously presented) The apparatus of claim 14, wherein the mechanism that exchanges information comprises:

customer service management software that periodically sends event notifications and statistical information from the client software of the managed user to the management server.

25. (Original) The apparatus of claim 24 wherein the event notifications include error notifications.

26. (Original) The method of claim 24 wherein event notifications and statistical information are temporarily stored in a memory located at a client site.

27. (Currently Amended) At least one computer readable storage medium encoded with instructions, that are executable in a computer system to perform a method managing a peer-to-peer collaboration system, comprising acts of:

connecting a first user to a second user in a peer-to-peer collaboration session including the first and second users, the first user having a first collaboration identity in a shared space and the second user having a second collaboration identity in the shared space;

downloading from the management server to client software operating in the computer system a definition file containing a definition of a managed entity;

associating a management identity in the definition file with the first collaboration identity in the client software in order to create the managed entity, the management identity associated with the managed entity being different than the first collaboration identity, the management identity allowing the first user or computer system to be identified by the management server; and

interacting with the management server using the management identity to exchange information relating to the managed entity within a collaboration session using the shared space, wherein the exchanged management information comprises at least a ~~license file and/or a policy restriction file~~, and the interacting further comprises:

~~if the exchanged information includes a policy restriction file~~, in response to information in the policy restriction file, restricting at least one function in the client software, wherein interacting further comprises:

- i) creating a client list of policy restrictions in the client software of the managed user;
- ii) sending the client list to the management server;
- iii) creating a server list of policy restrictions in the management server;
- iv) comparing the client list to the server list; and
- v) adjusting and synchronizing the policy restrictions in the client software based on the comparison on step iv)

28. (Previously Presented) The at least one computer readable storage medium of claim 27 wherein the managed entity is a managed user and the definition file is an injectible identity file.

29. (Previously Presented) The at least one computer readable storage medium of claim 27 wherein the managed entity is a managed device and the definition file is a device information file.

30. (Previously Presented) The at least one computer readable storage medium of claim 29 wherein the device information file is a Windows REG file.

31. (Canceled).

32. (Previously Presented) The at least one computer readable storage medium of claim 27, wherein the program code for interacting comprises:

sending at least one policy restriction file from the management server to the managed user; and

responding to information in the policy restriction file for restricting at least one function in the client software.

33. (Previously Presented) The at least one computer readable storage medium of claim 27, wherein the program code for interacting comprises:

creating a client list of policy restrictions in the client software of the managed user;

sending the client list to the management server;

creating a server list of policy restrictions in the management server;

comparing the client list to the server list; and

cooperating with the comparing program code for adjusting and synchronizing the policy restrictions in the client software.

34.-35 (Canceled).

36. (Previously Presented) The at least one computer readable storage medium of claim 33 wherein the program code for adjusting and synchronizing the policy restrictions operates periodically.

37. (Previously Presented) The at least one computer readable storage medium of claim 27, wherein the program code for interacting comprises:

periodically sending event notifications and statistical information from the client software of the managed user to the management server.

38. (Previously Presented) The at least one computer readable storage medium of claim 37 wherein the event notifications include error notifications.

39. (Previously Presented) The at least one computer readable storage medium of claim 37 further comprising program code for temporarily storing event notifications and statistical information in a memory located at a client site.

40. (Canceled).

41. (Currently Amended) Apparatus for managing a peer-to-peer collaboration system in which users having identities are directly connected to each other in a collaboration session using a shared space by client software operating in devices and wherein the users can communicate with a management server using the client software, the apparatus comprising:

means operable in devices for connecting a first user having a first collaboration identity in the shared space to a second user having a second collaboration identity in the shared space in a peer-to-peer collaboration session including the first and second users;

means for downloading from the management server to the client software a definition file containing a definition of the identity of the managed entity;

means in the client software for associating the identity of the managed entity with the first collaboration identity or first device information in the client software in order to create the



managed entity, the management identity associated with the managed entity being different than the first collaboration identity, the management identity allowing the first user or first device to be identified by the management server;

means for exchanging management information associated with the managed entity using the management identity, the management information relating to the collaboration session, and the management information being exchanged between the client software and the management server, and the management information identifying an entity to which the information relates using the new identity of the managed entity, wherein the exchanged management information comprises at least ~~a license file and/or~~ a policy restriction file; and

means for restricting at least one function in the client software in response to information in the policy restriction file ~~if the exchanged information includes a policy restriction file.~~

42. (Previously presented) The apparatus of claim 41 wherein the managed entity is a managed user and the definition file is an injectible identity file.

43. (Previously presented) The apparatus of claim 41 wherein the managed entity is a managed device and the definition file is a device information file.

44. (Original) The apparatus of claim 43 wherein the device information file is a Windows REG file.

45. (Canceled).

46. (Previously presented) The apparatus of claim 41, wherein the means for exchanging management information comprises:

means for sending at least one policy restriction file from the management server to the managed user; and

means responsive to information in the policy restriction file for restricting at least one function in the client software.

47. (New) The apparatus of claim 14, wherein:  
the exchanged management information comprises a license file; and  
the apparatus is adapted to, in response to information in the in the license file, enable at least one function in the client software.
48. (New) The at least one computer readable storage medium of claim 27, wherein:  
the exchanged management information comprises a license file; and  
the interacting further comprises in response to information in the in the license file, enabling at least one function in the client software.
49. (New) The apparatus of claim 41, wherein:  
the exchanged management information comprises a license file; and  
the apparatus further comprises means for enabling at least one function in the client software in response to information in the in the license file.